

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
11 January 2001 (11.01.2001)

PCT

(10) International Publication Number  
WO 01/03398 A3

(51) International Patent Classification<sup>7</sup>: H04L 29/06 (74) Agent: LING, Christopher, John; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(21) International Application Number: PCT/GB00/02469 (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(22) International Filing Date: 28 June 2000 (28.06.2000) (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(25) Filing Language: English (26) Publication Language: English

(30) Priority Data: 09/343,454 30 June 1999 (30.06.1999) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant (for MC only): IBM UNITED KINGDOM LIMITED [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventors: BELLWOOD, Thomas, Alexander; 14924 Coredero Drive, Austin, TX 78717 (US). LITA, Christian; 11101 Appletree Lane, Austin, TX 78726 (US). RUTKOWSKI, Matthew, Francis; 816 Clarence Bohls Lane, Pflugerville, TX 78660 (US).

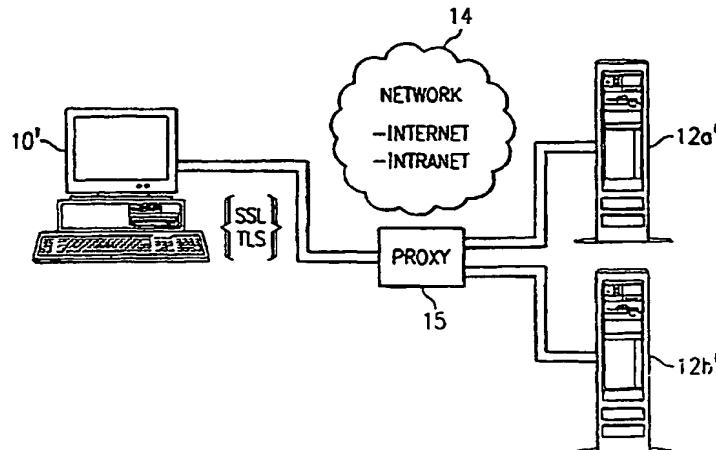
Published:

— With international search report.

(88) Date of publication of the international search report: 7 June 2001

[Continued on next page]

(54) Title: DYNAMIC CONNECTION TO MULTIPLE ORIGIN SERVERS IN A TRANSCODING PROXY



WO 01/03398 A3

(57) Abstract: A method of enabling a proxy to participate in a secure communication between a client and a set of servers. The method begins by establishing a first secure session between the client and the proxy. Upon verifying the first secure session, the method continues by establishing a second secure session between the client and the proxy. In the second secure session, the client requests the proxy to act as a conduit to a first server. Thereafter, the client and the first server negotiate a first session master secret. Using the first secure session, this first session master secret is then provided by the client to the proxy to enable the proxy to participate in secure communications between the client and the first server. After receiving the first session master secret, the proxy generates cryptographic information that enables it to provide a given service (e.g., transcoding) on the client's behalf and without the first server's knowledge or participation. If data from a second server is required during the processing of a given client request to the first server, the proxy issues a request to the client to tunnel back through the proxy to the second server using the same protocol.

(19)日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表2003-503963

(P2003-503963A)

(43)公表日 平成15年1月28日 (2003.1.28)

(51)Int.Cl. <sup>1</sup>	識別記号	F I	マーク <sup>2</sup> (参考)
H 04 L 9/08		G 06 F 13/00	5 10 A 5 B 0 8 5
G 06 F 13/00	5 1 0	15/00	3 1 0 D 5 J 1 0 4
15/00	3 1 0	H 04 L 12/22	5 K 0 3 0
H 04 L 12/22		12/66	B
12/66		9/00	6 0 1 C

審査請求 有 予備審査請求 有 (全 35 頁) 最終頁に続く

(21)出願番号	特願2001-508136(P2001-508136)
(36) (22)出願日	平成12年6月28日 (2000.6.28)
(35)翻訳文提出日	平成13年12月26日 (2001.12.26)
(36)国際出願番号	PCT/GB00/02469
(37)国際公開番号	WO01/003398
(37)国際公開日	平成13年1月11日 (2001.1.11)
(31)優先権主張番号	09/343,454
(32)優先日	平成11年6月30日 (1999.6.30)
(33)優先権主張国	米国 (US)

(71)出願人 インターナショナル・ビジネス・マシーンズ・コーポレーション  
INTERNATIONAL BUSINESS MACHINES CORPORATION  
アメリカ合衆国10504、ニューヨーク州  
アーモンク ニュー オーチャード ロード  
(72)発明者 ベルウッド、トーマス、アレクサンダー  
アメリカ合衆国78717 テキサス州オース  
チン コレデロ・ドライブ 14924  
(74)代理人 弁理士 坂口 博 (外1名)

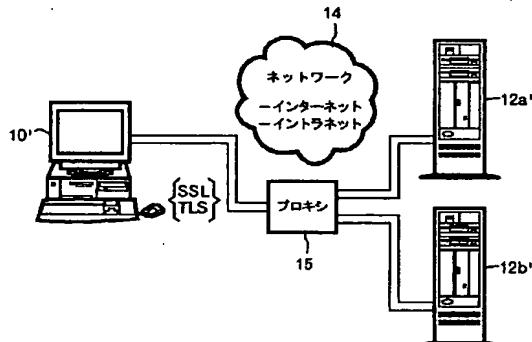
最終頁に続く

(54)【発明の名称】 トランスコーディング・プロキシでの複数の起点サーバへの動的接続

(57)【要約】

【課題】 プロキシが、クライアントとサーバの組の間のセキュア通信に参加できるようにする方法を提供すること。

【解決手段】 この方法は、クライアントとプロキシの間で第1セキュア・セッションを確立することによって開始される。第1セキュア・セッションを検証した後に、この方法は、クライアントとプロキシの間の第2セキュア・セッションを確立することによって継続される。第2セキュア・セッションでは、クライアントが、第1サーバへのコンジットとして働くようにプロキシに要求する。その後、クライアントと第1サーバが、第1セッション・マスター・シークレットをネゴシエーションする。第1セキュア・セッションを使用して、この第1セッション・マスター・シークレットが、クライアントによってプロキシに提供されて、プロキシが、クライアントと第1サーバの間のセキュア通信に参加できるようになる。第1セッション・マスター・シークレットを受信した後に、プロキシは、クライアントの代わりに、第1サーバの知識または参加なしで、所与のサービス (たとえ



**【特許請求の範囲】****【請求項1】**

プロキシ(15)がクライアント(10')と第1起点サーバ(12a')との間のセキュア通信に参加できるようにする方法であって、

(a) 前記クライアントと前記プロキシとの間の第1セキュア・セッションを確立するステップ(20、22)と、

(b) 前記第1セキュア・セッションを検証した後に、前記クライアントと前記プロキシとの間の第2セキュア・セッションであって、前記プロキシに前記第1起点サーバへのコンジットとして働くことを要求する第2セキュア・セッションを確立するステップ(24、26)と、

(c) 前記クライアントおよび前記第1起点サーバに、セッション・マスター・シークレットをネゴシエーションさせるステップ(30)と、

(d) 前記プロキシが前記セキュア通信に参加できるようにするために、前記第1セキュア・セッションを使用して、前記クライアントに前記セッション・マスター・シークレットを前記プロキシに配送させるステップ(32)と、

(e) 前記第1起点サーバに対するクライアント要求に応答して、前記プロキシが第2起点サーバへのコンジットとして働くことができるようるためにステップ(a)および(b)を繰り返すステップと、

(f) 前記クライアントおよび前記第2起点サーバに新しいセッション・マスター・シークレットをネゴシエーションさせるステップと、

(g) クライアントに、ステップ(e)で生成された前記第1セキュア・セッションを使用して前記プロキシに前記新しいセッション・マスター・シークレットを配送させるステップと

を含む方法。

**【請求項2】**

さらに、所与の暗号情報を生成するために、前記プロキシ(15)に、前記セッション・マスター・シークレットおよび前記新しいセッション・マスター・シークレットを使用させるステップを含む、請求項1に記載の方法。

**【請求項3】**

さらに、前記プロキシ(15)に、ステップ(d)の前記セッション・マスター・シークレットの受信の後にアクティブ動作状態に入らせるステップを含む、請求項2に記載の方法。

【請求項4】

前記プロキシ(15)が、前記アクティブ動作状態で前記クライアント(10')の代わりに所与のサービスを実行する、請求項3に記載の方法。

【請求項5】

前記所与のサービスがトランスコーディングである、請求項4に記載の方法。

【請求項6】

前記第1セキュア・セッションおよび前記第2セキュア・セッションが、ネットワーク・セキュリティ・プロトコルに準拠する、請求項1に記載の方法。

【請求項7】

前記サーバ(12a')が、ウェブ・サーバであり、前記クライアント(10')が、パーベイシブ・コンピューティング・クライアントである、請求項1に記載の方法。

【請求項8】

プロキシ(15)がクライアント(10')とサーバ(12a')との間のセキュア通信に参加できるようにする方法であって、

(a) 1から「n」台のサーバの組のそれぞれについて、

(1) 前記クライアントに、前記プロキシへの第1セキュア接続を要求させるステップ(20、22)と、

(2) 前記プロキシから受信する証明書の有効性を認証した時に、前記クライアントに、前記プロキシへの第2セキュア接続を要求させるステップ(24、26)であって、前記第2セキュア接続が、前記サーバへのコンジットとして働くように前記プロキシに要求する、ステップと、

(3) 前記クライアントおよび前記サーバに、前記コンジットを介して各々のセッション・マスター・シークレットをネゴシエーションさせるステップ(30)と、

(4) 前記ネゴシエーションの完了時に、前記クライアントに、前記第1セキ

ュア接続を使用して前記プロキシに前記各々のセッション・マスター・シークレットを配送させるステップ(32)と

(b) 前記プロキシに、前記セキュア通信への参加に有用な所与の暗号情報を生成するために前記各々のセッション・マスター・シークレットを使用させるステップと

を含む方法。

【請求項9】

さらに、前記プロキシ(15)に、前記クライアントの代わりに所与のサービスを実行させるステップを含み、前記所与のサービスが、トランスコーディング、キャッシング、暗号化、暗号化解除、監視、フィルタリング、および事前取出しを含むサービスの組から選択される、請求項8に記載の方法。

【請求項10】

プロキシ(15)がセキュア通信に参加できるようにする方法であって、

(a) 第1セキュア・セッションを確立するためにクライアントから前記プロキシに要求を送信するステップ(20)と、

(b) 前記クライアントと前記プロキシとの間の第2セキュア・セッションを確立するために前記クライアントから前記プロキシに要求を送信するステップ(24)であって、前記第2セキュア・セッションが、起点サーバへのコンジットとして働くように前記プロキシに要求する、ステップと、

(c) 前記プロキシが前記セキュア通信に参加できるようにするために、前記第1セキュア・セッションを使用して前記クライアントから前記プロキシにセッション・マスター・シークレットを送信するステップ(32)と、

(d) 前記プロキシからの要求の前記クライアントでの受信に応答して、前記プロキシがもう1つの起点サーバへのコンジットとして働くようにするために、ステップ(a)および(b)を繰り返すステップと、

(e) 前記クライアントから前記プロキシに新しいセッション・マスター・シークレットを送信するステップと

を含む方法。

【請求項11】

前記新しいセッション・マスタ・シークレットが、前記第1セキュア・セッションを介して送信される、請求項10に記載の方法。

【請求項12】

プロキシ(15)がセキュア通信に参加できるようにする方法であって、

(a) クライアントと前記プロキシとの間で第1セキュア・セッションを確立するために、前記クライアントからの要求を前記プロキシで受信するステップ(20)と、

(b) 前記クライアントと前記プロキシとの間の第2セキュア・セッションを確立するために、前記クライアントからの要求を前記プロキシで受信するステップ(24)であって、前記第2セキュア・セッションが、前記プロキシが起点サーバへのコンジットとして働くように要求する、ステップと、

(c) 前記第1セキュア・セッションを使用して前記クライアントから送信されるセッション・マスタ・シークレットを、前記プロキシで受信するステップ(32)と、

(d) 前記プロキシから前記クライアントへの所与の要求の送信時に、前記プロキシがもう1つの起点サーバへのコンジットとして働くようにするために、ステップ(a)から(c)までを繰り返すステップと、

(e) 前記クライアントから送信された新しいセッション・マスタ・シークレットを前記プロキシで受信するステップと  
を含む方法。

【請求項13】

さらに、所与の暗号情報を生成するために、前記プロキシ(15)に、前記セッション・マスタ・シークレットおよび前記新しいセッション・マスタ・シークレットを使用させるステップを含む、請求項12に記載の方法。

【請求項14】

プロキシ(15)がクライアント(10')と第1起点サーバ(12a')との間のセッションに参加できるようにする方法であって、

前記プロキシを介して、第1セッション鍵を作るために、前記クライアントと前記第1起点サーバとの間でセキュリティ・ハンドシェーク手順を行うステップ

(20、22、24、26、30)と、

前記プロキシが前記セッション中に前記クライアントと前記第1起点サーバとの間の通信に参加できるようにするために、前記クライアントに前記第1セッション鍵を前記プロキシに送信させるステップと、

前記セッションが進行する際に、第2セッション鍵を作るために前記クライアントと第2起点サーバとの間でセキュリティ・ハンドシェーク手順を行うステップと、

前記プロキシが前記クライアントによる前記第1起点サーバへの要求をサービスする際に使用するために前記第2起点サーバからデータを得られるようにするために、前記クライアントに前記第2セッション鍵を前記プロキシに送信させるステップと

を含む方法。

#### 【請求項15】

各セッション鍵が、異なるセキュア接続を介して前記クライアント(10')から前記プロキシ(15)に送信される、請求項14に記載の方法。

#### 【請求項16】

各セッション鍵が、同一のセキュア接続を介して前記クライアント(10')から前記プロキシ(15)に送信される、請求項14に記載の方法。

#### 【請求項17】

暗号システムであって、

クライアント(10')と、

サーバの組(12a'、12b')と、

プロキシ(15)と、

前記クライアントおよび各サーバがセキュア接続を介して通信できるようにするネットワーク・プロトコル・サービスと、

(i) 前記プロキシへの第1セキュア接続を要求するように前記クライアントを制御し、(ii) 前記プロキシからの証明書の有効性の検証に応答して、前記プロキシへの第2セキュア接続であって、前記プロキシに所与のサーバへのコンジットとして働くように要求する第2セキュア接続を要求するように前記クライ

アントを制御し、(i i i) セッション・マスタ・シークレットを得るために、前記コンジットを介して前記所与のサーバとネゴシエーションするように前記クライアントを制御し、(i v) 前記ネゴシエーションの成功裡の完了時に、前記第1セキュア接続を使用して前記プロキシに前記セッション・マスタ・シークレットを配送するように前記クライアントを制御する、コンピュータ・プログラムと、

(i) 所与の暗号情報を生成するために前記セッション・マスタ・シークレットを使用するように前記プロキシを制御し、(i i) 前記クライアントがもう1つのサーバとの別のセキュア接続を選択的に確立することを要求するように前記プロキシを制御し、(i i i) その間に前記プロキシが前記クライアントと前記所与のサーバとの間の通信に参加することができるアクティブ動作状態に前記プロキシを切り替える、コンピュータ・プログラムと  
を含む、暗号システム。

#### 【請求項18】

前記プロキシ(15)が、前記クライアント(10')の代わりにトランスコーディング・サービスを提供する手段を含む、請求項17に記載の暗号システム。

#### 【請求項19】

前記プロキシ(15)が、前記クライアント(10')の代わりに暗号化／暗号化解除サービスを提供する手段を含む、請求項18に記載の暗号システム。

#### 【請求項20】

前記プロキシ(15)が、前記クライアント(10')の代わりにキャッシング・サービスを提供する手段を含む、請求項17に記載の暗号システム。

#### 【請求項21】

前記プロキシ(15)が、前記クライアント(10')の代わりに監視サービスを提供する手段を含む、請求項17に記載の暗号システム。

#### 【請求項22】

クライアント(10')、サーバの組(12a'、12b')、およびプロキシ(15)を含む暗号システムで使用される、コンピュータ可読媒体内のコンピ

ュータ・プログラム製品であって、

(i) 前記プロキシへの第1セキュア接続を要求するように前記クライアントを制御し、(ii) 前記プロキシからの証明書の有効性の検証に応答して、プロキシへの第2セキュア接続であって、前記プロキシに所与のサーバへのコンジットとして働くように要求する第2セキュア接続を要求するように前記クライアントを制御し、(iii) セッション・マスタを得るために、前記コンジットを介して前記所与のサーバとネゴシエーションするように前記クライアントを制御し、(iv) 前記ネゴシエーションの成功裡の完了時に、前記第1セキュア接続を使用して前記プロキシに前記セッション・マスタ・シークレットを配送するよう前記クライアントを制御する、第1ルーチンと、

(i) 所与の暗号情報を生成するために前記セッション・マスタ・シークレットを使用するように前記プロキシを制御し、(ii) 前記クライアントがもう1つのサーバとの別のセキュア接続を選択的に確立することを要求するように前記プロキシを制御し、(iii) その間に前記プロキシが前記クライアントと前記所与のサーバとの間の通信に参加することができるアクティブ動作状態に前記プロキシを切り替える、第2ルーチンと

を含むコンピュータ・プログラム製品。

### 【請求項23】

プロキシ(15)がセキュア通信に参加できるようにするためにクライアント(10')内で使用される、使用可能媒体上のコンピュータ可読プログラム・コードを有するコンピュータ・プログラム製品であって、

第1セキュア・セッションを確立するために、前記クライアントから前記プロキシへ要求を送信する手段と、

前記クライアントと前記プロキシとの間の第2セキュア・セッションであって、前記プロキシが起点サーバへのコンジットとして働くように要求する第2セキュア・セッションを確立するために、前記クライアントから前記プロキシへ要求を送信する手段と、

前記プロキシが前記セキュア通信に参加できるようにするために、前記第1セキュア・セッションを使用して前記クライアントから前記プロキシにセッション

・マスタ・シークレットを送信する手段と、  
新しいセッション・マスタ・シークレットを得るように前記クライアントを制  
御するために、前記セキュア通信中に前記プロキシからの所与の要求のクライア  
ントでの受信に応答する手段と、  
前記クライアントから前記プロキシに前記新しいセッション・マスタ・シーク  
レットを送信する手段と  
を含むコンピュータ・プログラム製品。

【請求項24】

プロキシ(15)がセキュア通信に参加できるようにするために前記プロキシ  
内で使用される、使用可能媒体上のコンピュータ可読プログラム・コードを有す  
るコンピュータ・プログラム製品であって、

前記クライアントと前記プロキシとの間で第1セキュア・セッションを確立す  
るために、前記クライアントからの要求を前記プロキシで受信する手段と、

前記クライアントと前記プロキシとの間の第2セキュア・セッションを確立す  
るために、前記クライアントからの要求を前記プロキシで受信する手段であって  
、前記第2セキュア・セッションが、前記プロキシが起点サーバへのコンジット  
として働くことを要求する、手段と、

前記第1セキュア・セッションを使用して前記クライアントから送信されるセ  
ッション・マスタ・シークレットを、前記プロキシで受信する手段と、

前記プロキシから前記クライアントへ所与の要求を送信するための前記セキュ  
ア通信中の所与のオカレンスに応答する手段と、

前記クライアントから送信された新しいセッション・マスタ・シークレットを  
前記プロキシで受信する手段と  
を含むコンピュータ・プログラム製品。

【請求項25】

さらに、所与の暗号情報を生成するために前記セッション・マスタ・シークレ  
ットおよび前記新しいセッション・シークレットを使用する手段を含む、請求項  
24に記載のコンピュータ・プログラム製品。

**【発明の詳細な説明】****【0001】****【発明の属する技術分野】**

本発明は、全般的にはネットワーク・セキュリティ・プロトコルに関し、具体的には、クライアントと1つまたは複数の起点サーバの間のセキュア・セッションのプライバシを仲介物（たとえばトランスコーディング・プロキシ）に拡張する方法に関する。

**【0002】****【従来の技術】**

Netscape社のSecure Sockets Layerプロトコル（SSL）およびInternet Engineering Task Force（IETF）Transport Layer Securityプロトコル（TLS）などのネットワーク・セキュリティ・プロトコルが、通信アプリケーション間のプライバシおよびデータ保全性を提供する。たとえば、これらのプロトコルは、インターネットを介する電子商取引トランザクションの保護に一般に使用されている。

**【0003】**

最近、コンピュータ産業が、通常は従来のコンピュータとみなされるはずのもの以外の装置にコンピュータ処理機能および通信機能を追加しようとしてきた。そのような装置は、非常にさまざまであり、たとえば、携帯情報端末（PDA）、ビジネス・オーガナイザ（たとえばIBM（登録商標）WorkPad（登録商標）および3Com（登録商標）PalmPilot（登録商標））、スマートホン、セル電話、他のハンドヘルド・デバイス、および類似物が含まれる。便宜上、これらの装置を、1つの種類として、「パーセイシブ・コンピューティング」クライアントと称する場合がある。というのは、これらが、コンピュータ・ネットワークのサーバに接続され、その位置に関わりなくコンピューティングの目的に使用されるように設計されるからである。

**【0004】**

しかし、パーセイシブ・コンピューティング・クライアントは、通常は、Hewlett-Packard（登録商標）ベース・クライアントのすべての機能セットをサ

ポートしない。その結果、トランスコーディング・サービスが、通常は、バーベイシブ・クライアントでレンダリングされる情報を、あるソース・マークアップ言語（たとえばHTML）から別の言語（たとえばHDMLまたはハンドヘルド・デバイス・マークアップ言語）に変換する必要がある。しかし、セキュア・ネットワーク接続を介するトランスコーディング・サービスの提供は、問題がある。具体的に言うと、SSLおよびTLSなどの従来のセキュリティ・プロトコルが、まさにクライアントとサーバの間の通信に第三者が介入することを防止するために設計されているので、セキュリティとトランスコーディング・サービスの間に根本的な衝突がある。

#### 【0005】

セキュア・セッションで第三者の介入を制限することは、他のアプリケーションでも問題がある。たとえば、クライアントがファイヤウォールの背後に配置される場合に、外部ネットワークのサーバへのSSL/TLS通信を、簡単に監査または他の形で監視することができない。したがって、データ・レコードまたは他の機密情報が、おそらくは管理許可なしでクライアントから送信される可能性がある。もう1つの例として、セキュア接続を介してサーバと通信するクライアントは、そうでなければネットワーク・リソースの需要を減らし、装置間の通信を機能強化するのに役立つはずの、第三者のキャッシング機構または事前取出し機構を利用することができない。

#### 【0006】

##### 【発明が解決しようとする課題】

プロキシがネットワーク・プロトコルのセキュリティを滅殺せずに所与の機能（たとえばトランスコーディング、監査、監視、キャッシング、事前取出し、クライアントの代わりの暗号化／暗号化解除など）を実行できるようにするために、クライアントがプロキシに十分なセキュリティ情報を委任できるようにする機構を提供することが望ましい。さらに、そのようなプロキシが、クライアントの代わりに要求をサービスする処理中に、別の起点サーバからのデータを保護できるようにすることも望ましい。

#### 【0007】

**【課題を解決するための手段】**

起点サーバと通信するのにネットワーク・セキュリティ・プロトコル（たとえばSSLまたはTLS）を使用しているクライアントが、セッションのセキュリティ属性を変更せずに、プロキシがセッションに参加することを可能にする。本発明によれば、クライアントが、起点サーバとネゴシエーションされたセッション・マスタ・シークレットをとり、そのシークレットをプロキシにセキュアに配達できるようにするプロトコルが提供される。プロキシは、そのマスタ・シークレットを使用して、クライアントとサーバの間で渡されるデータの暗号化／暗号化解除を行う。プロキシが、所与のクライアント要求をサービスしている間に第2の起点サーバからの追加のセキュア・データを必要とする場合には、プロキシは、クライアントに、もう1つのセッション・マスタ・シークレット（第2の起点サーバとネゴシエーションされた）を得るためにそのプロトコルを繰り返すよう求め、このシークレットが、その後、第2の起点サーバからデータを得る際に使用するためにプロキシに配達される。

**【0008】**

本発明によれば、所与の第三者の仲介物またはプロキシが、クライアントと1つまたは複数の起点サーバとの間のセキュア・セッションに参加できるようになる。第三者が、所与の起点サーバの明示された知識なしで参加することが好ましい。その結果、この方法は、起点サーバに対する変更も、セッション・シークレットをネゴシエーションする際に使用されるハンドシェーク・プロトコルに対する変更も必要としない。

**【0009】**

本発明によれば、ネットワーク・セキュリティ・プロトコルに従って通信が受け渡される間にセキュリティ・サービスおよび他のサービス（たとえば、トランスコーディング、キャッシング、監視、クライアントの代わりの暗号化／暗号化解除、および類似物）が共存できるようになる。

**【0010】**

具体的に言うと、本発明によれば、パーオペイシブ・コンピューティング・クライアントがセキュア・リンクを介して1つまたは複数の起点サーバと通信する間

に、プロキシがトランスコーディング・サービスを提供できるようになる。

【0011】

本発明によれば、プロキシが、ネットワーク・セキュリティ・プロトコルを使用して1つまたは複数のサーバと通信するクライアントの代わりに、キャッシングまたは他の管理サービスを実行できるようになる。

【0012】

本発明によれば、プロキシが、ネットワーク・サーバ・プロトコルを使用して1つまたは複数の起点サーバと通信するクライアントの代わりに、暗号化／暗号化解除を実行できるようになる。

【0013】

好ましい実施形態では、プロキシが、クライアントと第1サーバの間のセキュア通信に参加する。この方法は、クライアントとプロキシの間で第1セキュア・セッションを確立することによって開始される。第1セキュア・セッションを検証した後に、この方法は、クライアントとプロキシの間の第2セキュア・セッションを確立することによって継続される。第2セキュア・セッションでは、クライアントが、第1サーバへのコンジットとして働くようにプロキシに要求する。その後、クライアントと第1サーバが、第1セッション・マスタ・シークレットをネゴシエーションする。第1セキュア・セッションを使用して、この第1セッション・マスタ・シークレットが、クライアントによってプロキシに提供され、プロキシが、クライアントと第1サーバの間のセキュア通信に参加できるようになる。第1セッション・マスタ・シークレットを受信した後に、プロキシは、クライアントの代わりに、サーバの知識または参加なしで、所与のサービス（たとえばトランスコーディング、監視、暗号化／暗号化解除、キャッシング、および類似物）を提供できるようになるための暗号情報を生成する。第1セキュア・セッションは、そのような通信中に、クライアントとプロキシの間で維持される。

【0014】

本発明の特徴によれば、プロキシが、所与のクライアント要求を処理するため第2サーバからのデータを必要とする場合に、上で述べたプロトコルが繰り返

される。具体的に言うと、プロキシが、やはりプロキシを介してトンネリングすることによって第2サーバとの別の接続を確立する要求をクライアントに発行する。上で述べたように、このプロトコルによって、クライアントが、第2サーバとの第2セッション・マスター・シークレットを確立できるようになり、そのシークレットが、前に説明した形でプロキシと共用される。プロキシは、この第2シークレットを使用して第2サーバからセキュア・データを得ることによって、そのサービス動作（たとえばトランスコーディング）を継続する。

#### 【0015】

したがって、基本的なトンネリング・プロトコルが、クライアントと所与の起点サーバの間で確立された後に、クライアントがこのプロトコルを必要に応じて繰り返して、プロキシが、所与の起点サーバに対する所与のクライアント要求をサービスしながら、「n」個までの追加の起点サーバからセキュア・データを得ることができる。

#### 【0016】

これから、本発明を、図面を参照して、例としてのみ説明する。

#### 【0017】

##### 【発明の実施の形態】

図1に、従来技術の通常のクライアント/サーバ・ネットワーク・アーキテクチャを示す。この図では、クライアント10が、ネットワーク14を介してサーバ12と通信し、このネットワーク14は、インターネット、イントラネット、広域ネットワーク、ローカル・エリア・ネットワーク、または類似物とすることができます。クライアント10およびサーバ12は、Netscape社のSecure Socket Layer (SSL) プロトコルまたはIETFのTransport Layer Security (TLS) プロトコルなどのネットワーク・セキュリティ・プロトコルを使用して通信する。一般化すると、クライアントは、サーバへのTLS接続またはSSL接続を開始するアプリケーション実体である。サーバは、応答を送り返すことによって要求にサービスするための接続を受け入れるアプリケーション実体またはプログラムである。所与のどのプログラムでも、クライアントとサーバの両方になることができる。サーバとクライアントの間の主な動作の差は、サーバが、一般に

認証され、クライアントが、任意選択としてのみ認証されることである。所与のリソースが存在するか作成されるサーバを、本明細書では、時々、起点サーバと称する。

#### 【0018】

クライアント10およびサーバ12は、セキュア・セッションに参加する。SSLセッションまたはTLSセッションは、ハンドシェーク・プロトコルによって作成される、クライアントとサーバの間の関連である。セッションによって、複数の接続にまたがって共用することができる暗号セキュリティ・パラメータの組が定義される。これらは、接続ごとの新しいセキュリティ・パラメータの高価なネゴシエーションを防ぐのに使用される。SSLまたはTLSでは、セッション識別子が、特定のセッションを識別する、サーバによって生成される値である。SSLセッションまたはTLSセッションを確立するために、クライアントとサーバが、ハンドシェークを実行するが、このハンドシェークは、実体の間のトランザクションのパラメータを確立する初期ネゴシエーションである。セッションが作成された後に、クライアントとサーバの間の通信が、接続を介して行われ、この接続は、適当なタイプのサービスを提供するトランスポート(OSI階層化モデル定義での)である。SSLおよびTLSの場合、そのような接続は、対等関係である。接続は、一時的であり、すべての接続が、1つのセッションに関連する。通常、接続を介する通信は、公開鍵暗号を使用して保護され、公開鍵暗号は、2つの鍵の暗号を使用する暗号技法の種類である。公開鍵を用いて暗号化されたメッセージは、関連する秘密鍵を用いなければ暗号化解除できない。逆に、秘密鍵を用いて署名されたメッセージを、公開鍵を用いて検証することができる。

#### 【0019】

セッションが確立された後に、クライアントは、証明書を有し、この証明書は、起点サーバに対してクライアントを認証するために、起点サーバによって発行されたものである。クライアントは、起点サーバを有効として認証できるようにするために、起点サーバに証明書を提示することも要求する。認証とは、ある実体が別の実体の識別を判定する能力である。通常、X.509プロトコル(別名

ISO認証フレームワーク)の一部として、証明書は、信頼される認証局によって割り当てられ、当事者の識別(または他の属性)とその公開鍵の間の強い束縛を提供する。

#### 【0020】

上で説明した機能性は、従来技術で既知である。この機能性は、たとえば、IETF TLS Version 1.0およびSSL Version 2.0/3.0に準拠するプロトコルで実施される。これらのプロトコルは、非常に類似しているが、レコード・プロトコルおよびハンドシェーク・プロトコルという2つの層からなる。後で説明するように、本発明は、セッションのプライバシを第三者の仲介物またはプロキシに拡張するためにこれらのタイプのセキュリティ・プロトコルを拡張する方法を利用する。本発明は、後で説明するように、セキュア・セッションの上位に階層化される、クライアントとプロキシの間のハンドシェーク・プロトコルと共に実施されることが好ましい。この拡張では、レコード・プロトコル層でのセキュア接続の基本特性が変更されない。この技法を、TLSおよびSSLに関して説明するが、これは、本発明の制限ではない。

#### 【0021】

図2を参照すると、基本的な方法によって、1つまたは複数の起点サーバ12'、a～nと通信するのにセキュリティ・プロトコルとしてSSLまたはTLSを使用しているクライアント10'が、セッションのセキュリティ属性を変更せずに、プロキシ15がセッションに参加することを可能にできるようになる。上で注記したように、この方法は、暗号強度または、クライアント10'および所与の起点サーバ12'が互いを認証するのに使用されるステップからの独立である。本発明は、プロトコルを拡張しながら、上位レベル・プロトコルをその上に階層化することができるという点で、TLS/SSLと同一の長所を有する。そのような上位レベル・プロトコルには、たとえば、通常はトランスポート(たとえばTCP/IP)層の真上の層であるアプリケーション・プロトコル(たとえばHTTP、TELNET、FTP、およびSMTP)が含まれる。

#### 【0022】

図3および図4は、本発明に有用なセキュリティ委任プロトコルの動作を示す

流れ図である。このプロトコルによれば、クライアント10'は、所与の起点サーバとの接続の確立を望むたびに、2つの別個のセッションをセット・アップする。第1セキュア・セッションは、クライアント10'とプロキシ15の間でセット・アップされ、このセッションは、クライアントとプロキシの間でシークレット情報を渡すためのパイプまたはコンジットとして使用される。第1セキュア・セッションは、この流れ図の最初の2列によって表される。さらに、クライアント10は、この流れ図の最後の3列によって表される、プロキシとの第2セキュア・セッションもセット・アップするが、このセッションでは、プロキシ15が、起点サーバ12'へのトンネリングに使用される。トンネルとは、2つの接続の間のブラインド・リレーとして働く仲介プログラムである。活動状態になった後に、トンネルは、所与の通信（たとえば、HTTP要求またはHTTP応答）の当事者とは見なされないが、トンネルが、その通信によって開始された可能性がある。

#### 【0023】

この例示的な例では、クライアントが、起点サーバ（時々第1サーバと称する）にアクセスして、所与のコンテンツを取り出すことを望むが、プロキシを使用して、これらのコンテンツを正しく表示することを望むと仮定する。要求のサービスで、1つまたは複数の追加の起点サーバから所与のオブジェクトを取り出すことが必要になる場合もある。上で注記したように、SSL/TLSプロトコルに従って、クライアントは、起点サーバに対してそのクライアントを認証するために起点サーバによって発行された証明書を有し、クライアントは、起点サーバを有効として認証できるようにするために、起点サーバに証明書を提示することも要求する。後で説明するように、クライアントは、クライアントがセッション・マスター・シークレットを（プロキシに）明かす前に、プロキシが証明書をクライアントに認証させることも要求する。

#### 【0024】

このルーチンは、ステップ20で、クライアントがプロキシとのセキュア・セッションを要求することによって開始される。これは、上で識別された第1セキュア・セッションである。流れ図からわかるように、クライアントは、そのセキ

ユリティ属性を委任しようとしているので、プロキシに証明書を要求しなければならない。これは、クライアントが、起点サーバのネゴシエーションされたシークレットを、内部セッション識別子と共に（プロキシに）送信する主セッションである。通常、この識別子は、SSL/TLSセッション識別子と同一ではない。これについては、後のステップで詳細に説明する。

#### 【0025】

ステップ22で、クライアントは、プロキシから受信した証明書の有効性を認証し、その結果、プロキシとのセキュア・セッションを有することに満足する。このルーチンは、ステップ24で継続されて、クライアントが、プロキシへの第2接続をオープンする。これは、上で説明した第2セキュア・セッションである。前に注記したように、クライアントは、所与の起点サーバへのトンネリングを要求する（たとえば、要求に関してHTTP CONNECTメソッドを使用する）。プロキシを介するトンネル要求の一部として、クライアントは、内部セッション識別子を生成しなければならないことをプロキシに通知するヘッダをHTTP要求に追加する。このヘッダは、クライアントが、将来にプロキシにマスター・シークレットを転送する意図を有することを暗示する。

#### 【0026】

ステップ26で、プロキシが、一意の内部セッション識別子を生成し、この情報をクライアントに返す。内部セッション識別子の値が、セキュアHTTP応答に付加される。これは、クライアントが、セッション・マスター・シークレットをプロキシに転送する時に使用する値である。ステップ28で、プロキシが、起点サーバとの接続を確立し、クライアントと起点サーバの間でデータが流れることを可能にする。この時点で、プロキシは、トンネルのように振る舞う。プロキシは、後で説明するように、クライアントがセッション・マスター・シークレットを転送するまでは、「アクティブ・プロキシ」にならない。ステップ30で、クライアントが、起点サーバとのハンドシェークを実行して、セッション・マスター・シークレットをネゴシエーションする。

#### 【0027】

このルーチンは、ステップ32で継続される。この時点で、クライアントが、

内部セッション識別子をセッション・マスタ・シークレットと共に（プロキシに）送信する。この情報は、図示のように主セッションで送信される。ステップ34で、プロキシが、内部セッション識別子およびセッション・マスタ・シークレットを受信する。プロキシは、この情報を使用して、起点サーバ応答を暗号化解除するのに使用される必要な暗号情報を作り、サービスされるコンテンツを修正し、データを暗号化し、その後に、クライアントにデータを送信する。その後、プロキシは、起点サーバとの現在の接続に関して「アクティブ・プロキシ」に切り替わる。

#### 【0028】

ステップ36で、クライアントが、起点サーバ上のリソースに関するセキュアHTTP要求を送信する。任意選択として、ステップ38で、プロキシが、要求を暗号化解除し、必要に応じて修正し、新しい要求を暗号化し、それを起点サーバに送信することができる。ステップ40で、起点サーバが、要求を満足し、応答データをプロキシに送り返す。起点サーバが、プロキシの能動的な参加を意識すらしないことが好ましいことに留意されたい。ステップ42で、プロキシが、コンテンツを受信し、暗号化解除し、データを修正して、クライアントのトランスコーディングの必要を満足する。任意選択として、ステップ44で、プロキシが、追加データを得るか性能を高めるために起点サーバとの追加の接続を確立することができる（起点サーバがセッション再開始をサポートする場合）。複数の接続が確立される場合に、暗号化ブロック・チェーン（CBC）を使用して、暗号を調整する。プロキシが、このセッションの一部として追加接続を確立しない場合には、プロキシは、主セッションでセッション識別子と共に通知を送信することによって、暗号仕様変更についてクライアントに通知しなければならない。この処理は、ステップ46に示されており、クライアントが将来にこの起点サーバとのセッションを再開できるようにするのに必要である。

#### 【0029】

本発明によれば、プロキシは、最初の起点サーバへの所与のクライアント要求の処理中に、他の起点サーバへの追加のセキュア・セッションを要求することができる。したがって、たとえば、プロキシが、たとえば現在の要求をトランスコ

ーディングするために、他の起点サーバへの追加のセキュア・セッションを必要とする場合に、プロキシは、クライアントが必要な追加の起点サーバのそれぞれとの新しいセッションを確立することを要求する通知をクライアントに送信する。これは、全般的にステップ48に示されている。最後に、プロキシが、最後にトランスコーディングされたコンテンツを暗号化し、クライアントに送信する。これがステップ50である。

#### 【0030】

図5は、プロキシが他の起点サーバへの1つまたは複数の追加のセキュア・セッションを開始する方法を詳細に示す図である。この例では、クライアント10”が、前に説明した形で、トランスコーディング・プロキシ15”および第1起点サーバ12”と協力する。図からわかるように、セッション1は、クライアントがプロキシと確立する最初のセッションを表し、セッション2では、クライアントが第1起点サーバとのセキュア・セッションを確立する。この図に示されたステップ(1)～(12)は、図3および図4の流れ図で上で説明したステップに対応する。例示的トランスコーディング動作中に、プロキシ15”が、第2起点サーバ17”からのセキュア・データが必要であると判定した場合には、プロキシは、サーバ17”との第2接続を、具体的にはやはりこのプロキシを介してトンネリングすることによって、確立するようにクライアント10”に求める。これによって、クライアントが、第2サーバ17”とのマスタ・シークレットを確立できるようになる。後者のマスタ・シークレットを、クライアントがプロキシを介して第1起点サーバへトンネリングすることの結果として生成されたセッション・マスタ・シークレットと区別するために、時々、第2マスタ・シークレットと称する。具体的に言うと、図5のステップ(13)に、プロキシ15”がクライアント10”への要求を行うことが示されている。その後、ステップ(3)～(7)を、前に説明した形で第2起点サーバ17”について繰り返す。

#### 【0031】

プロキシ15”は、一方ではクライアントと、他方では各々の起点サーバとの間の通信を保護する必要に応じて、別々のマスタ・シークレットを維持する能力を有する。したがって、クライアントとプロキシは、元のクライアント要求のコ

ンテキスト内で、起点サーバ・セッションごとに1つの、別々のマスタ・シークレットを維持する。これによって、プロキシが、クライアントの代わりに、複数の起点サーバに関してデータにアクセスし、データを使用することが可能になる。所望されるならば、クライアントが、同一のセキュア・セッションを介して（たとえば図1に示されたセッション1）または異なるセキュア・セッションを使用することによって、プロキシにセッション・マスタ・シークレットを配達することができる。

#### 【0032】

おわかりのように、クライアント、所与の起点サーバ、およびプロキシのすべてが、マスタ・セッション・シークレットを共用する。具体的に言うと、クライアントおよび所与の起点サーバが、マスタ・セッション・シークレットについて合意した後に、そのシークレットが、前にクライアントとプロキシの間で作成されたセキュア・セッションを介してプロキシに供給される。別の形で言えば、クライアントが、主（すなわち第1の）セッション（クライアントとプロキシの間の）を確立した後に、このマスタ・セッション鍵を（プロキシに）渡す。しかし、起点サーバは、プロキシが作業を行っているか他の形でセキュア接続に参加していることを意識する必要がない（通常は意識しない）。

#### 【0033】

おわかりのように、このセキュリティ委任をサポートするのに必要な変更は、最小限であり、クライアントおよびプロキシだけに影響し、所与のクライアント要求を処理するのに必要になる可能性がある所与の起点サーバには影響しない。また、この方法は、クライアントがその秘密鍵または起点サーバに対してクライアントを認証するのに使用される方法に関する情報を明かすことを必要としない。さらに、クライアントは、起点サーバとの追加の接続を確立する能力を有するので、暗号仕様を変更するかセッションを打ち切ることができ、したがって、クライアントの代わりに起点サーバへの他の接続を確立するプロキシの能力が制限される。

#### 【0034】

必要な変更を要約すると、クライアントは、1つまたは複数の各々の起点サー

バとネゴシエーションされた1つまたは複数のセッション・マスタ・シークレットを持つ能力と、それらをプロキシに保護された形で配送する能力とを有する必要がある。プロキシは、クライアントのセッションへの参加を開始できるようにするために、クライアントのマスタ・シークレットから必要な暗号化情報を作ることができるものがある。上の方法は、セッション・シークレットのネゴシエーションに使用されるハンドシェーク・プロトコルに対する変更を全く必要としない。総合的なネットワーク・トラフィックに対する追加の負荷は、最小限である。というのは、クライアントがプロキシからのサービスを必要とする間に、クライアントとプロキシの間に1つの追加セッションがあるだけだからである。起点サーバに必要な変更はない。

#### 【0035】

クライアントとプロキシの間の主セッションは、到着するレコードごとにセッション識別子があるので、非同期と見なすことができる。クライアントからプロキシへの書込は、肯定応答が不要なので、クライアントへのプロキシの書込と独立に発生することができる。もちろん、基礎となるトランスポート層で、信頼性のある配送方法が実施されることが仮定される。新しい接続（追加の起点サーバへの）を確立する、クライアントに対するプロキシ要求では、null\*セッション識別子を使用することが好ましい。というのは、後に、クライアントがトンネリングを要求する時に、プロキシによってセッション識別子が割り当てられるからである。性能上の理由から、プロキシは、クライアントが所与の起点サーバと同期していないので、クライアントが完全な認証ハンドシェークを実行することを強制されるという条件で、暗号仕様変更についてクライアントに通知する必要はない。これは、起点サーバとの初期セッション確立中のクライアントに対するより大きいペイロードを暗示するが、プロキシが新しい接続を確立するか、所与の起点サーバまたは他の起点サーバへの追加の要求を送信する場合のチャッターが減る。

#### 【0036】

プロキシに関する多数の応用例がある。以下は、複数の代表的な例である。

#### 【0037】

プロキシのそのような使用の1つが、クライアントが暗号化／暗号化解除を実行するのに要求される、必要な計算能力の削減である。たとえば、クライアントがファイヤウォールの背後に配置される場合に、プロキシを使用して、クライアントが、認証ステップを1回だけ実行し、プロキシとの間で実際にデータを平文で送受信し、したがって、暗号化ペイロードをプロキシに移動することができる。代替案では、プロキシを使用して、実際のデータ・レコードを起点サーバと交換できるようになる前に、クライアントがセッション・シークレットを渡すことができるようになる（またはそれを要求する）ことによって、ファイヤウォール構成に監査機能を提供する。この場合、プロキシは、クライアントがそれ自体または起点サーバに関するプライベート／特権情報を配達することを要求する必要がない。もう1つの例では、プロキシを使用して、クライアントと起点サーバの間のセッションのセキュリティ特性を変更せずに、キャッシング・プロキシがセッションに参加できるようにすることによって、クライアント性能を改善することができる。その代わりに、プロキシを使用して、プロキシがクライアントの秘密鍵の明示的な知識を有することなく、クライアントの代わりに（後にセッションを再開始することによって）コンテンツを事前に取り出すことができる。この場合、プロキシは、たとえば、オフピーク時間中に、クライアントの購読の定期的更新を得ることができる。これらの例は、単に例示的であって、本発明の範囲を制限するものと解釈されなければならない。

#### 【0038】

したがって、上で注記したように、本発明のもう1つの応用例は、第三者が、パーソナル・コンピューティング・クライアント装置を用いるセキュア・セッションに参加できるようにすることである。代表的な装置には、x86ベース、PowerPC（登録商標）ベース、またはRISCベースであり、WindRiver VXWorks（商標）、QSSL QNXNeutrino（商標）、またはMicrosoft Windows（登録商標）CEなどのリアルタイム・オペレーティング・システムを含み、ウェブ・ブラウザを含むことができる、パーソナル・クライアントが含まれる。この応用例を、下で詳細に示す。

#### 【0039】

図6を参照すると、代表的なパーべイシブ・コンピューティング装置には、複数のコンポーネント、たとえばクライアント・アプリケーション・フレームワーク142、仮想計算機144、言語エンジン146、および業界供給のランタイム・オペレーティング・システム（RTOS）148を含む、クライアント・スタック140が含まれる。クライアント・アプリケーション・フレームワーク142には、通常は、ブラウザ150、ユーザ・インターフェース152、パーべイシブ・コンピューティング・クライアント・アプリケーション・クラス・ライブラリ154、標準Java（登録商標）クラス・ライブラリ156、および通信スタック158が含まれる。パーべイシブ・コンピューティング・クライアントは、接続サービス162を介してサーバ・プラットホーム160に接続される。

#### 【0040】

この下位レベルでは、接続サービス62に、圧縮機能および暗号化機能を提供するゲートウェイ164が含まれる。ゲートウェイによって、本発明の方法に従って拡張されたネットワーク・セキュリティ・プロトコルが実施される。接続サービス162の上位レベルは、トランスコーディング、フィルタリング、優先順位付け、および装置管理へのリンクなどの1つまたは複数の異なる機能を提供するプロキシ166である。

#### 【0041】

サーバ・プラットホーム160すなわち所与の起点サーバは、複数の異なるタイプとすることができます。プラットホーム160は、ウェブ/アプリケーション・サーバ170（同期式要求-応答型サーバ）またはデータ同期化サーバ172および174（非同期式キュー通信型サーバ）とすることができます。そのようなサーバ・タイプのそれぞれの基本機能が図示されている。代替案では、プラットホーム160を、LDAPディレクトリ/リポジトリ、認識および通知、ネットワーク管理、装置寿命サイクル管理、ユーザおよび装置登録、または請求などの追加サービスを提供する付加価値サーバとすることができます。

#### 【0042】

このセキュリティ委任プロトコルは、従来技術に対する多数の長所を提供する。上で述べたように、このプロトコル拡張は、レコード・プロトコル層でのセキ

ュア接続の基本特性を変更しない。さらに、プロキシへの接続は、プライベートであり、対称暗号（たとえば、DES、RC4など）を、データ暗号化に使用することができる。この対称暗号化の鍵は、接続ごとに一意に生成され、別のプロトコル（TLSまたはSSLのハンドシェーク・プロトコルなど）によってネゴシエーションされたシークレットに基づくことが好ましい。さらに、プロキシへの接続は、信頼性がある。メッセージ・トランスポートには、通常は、キー付きMACを使用するメッセージ保全性検査が含まれる。セキュア・ハッシュ関数（たとえばSHA、MD5など）を、MAC計算に使用することが好ましい。

#### 【0043】

このハンドシェーク・プロトコルは、複数の基本特性を有する接続セキュリティを提供する。ピアの識別は、非対称暗号すなわち公開鍵暗号（たとえばRSA、DSSなど）を使用して認証することができる。この認証は、任意選択することができるが、一般に、ピアの少なくとも1つについて要求される。さらに、共用されるシークレットのネゴシエーションは、セキュアである。ネゴシエーションされるシークレットは、盗聴者には入手不能であり、すべての認証される接続について、接続の中に自身を置くことができる攻撃者であってもシークレットを得ることができない。さらに、プロキシとのネゴシエーションは、信頼性がある。攻撃者は、通信の当事者に検出されずに、ネゴシエーションされる通信を変更することができない。

#### 【0044】

上でさらに述べたように、このセキュリティ・プロトコルを用いると、プロキシが、セッションの属性を変更せずに、クライアントと起点サーバの組との間のセキュア・セッションに参加できるようになる。この方法は、暗号強度または使用される認証技法から独立でもある。

#### 【0045】

本発明は、プロセッサ内で実行可能なソフトウェア内で、すなわち、コンピュータのランダム・アクセス・メモリに常駐するコード・モジュール内の命令の組（プログラム・コード）として、実施することができる。コンピュータによって要求されるまで、命令の組を、別のコンピュータ・メモリ、たとえば、ハード・

ディスクまたは取外し可能メモリに保管するか、インターネットまたは他のコンピュータ・ネットワークを介してダウンロードすることができる。

【0046】

さらに、説明したさまざまな方法は、ソフトウェアによって選択的に活動化または再構成される汎用コンピュータで便利に実施されるが、当業者は、そのような方法を、必要な方法ステップを実行するように構成された、ハードウェア、ファームウェア、またはより特殊化された装置で実行できることを諒解するであろう。

【図面の簡単な説明】

【図1】

ネットワーク・セキュリティ・プロトコルを使用する既知のクライアント／サーバ・ネットワーキング環境の簡略化された図である。

【図2】

第三者の仲介物またはプロキシがセキュア・セッションに参加する、クライアント／サーバ・ネットワーキング環境の簡略化された図である。

【図3】

基本トンネリング方法の詳細な流れ図の前半である。

【図4】

基本トンネリング方法の詳細な流れ図の後半である。

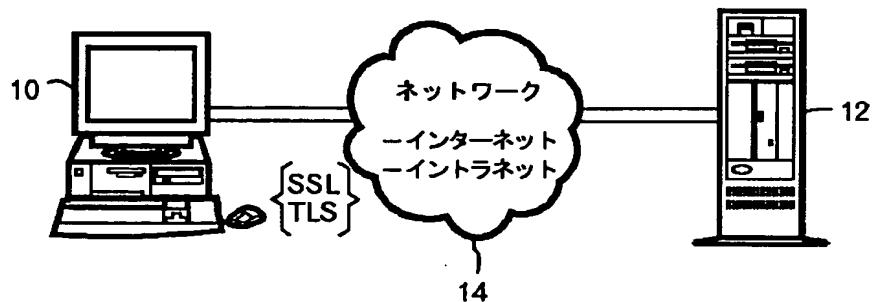
【図5】

クライアントがまずプロキシにセキュリティを委任した後に、プロキシが、プロキシを介して「n」個の追加の起点サーバへトンネリングすることによって、1つまたは複数の追加のセキュア接続を確立することをクライアントに要求する、本発明の簡略化されたブロック図である。

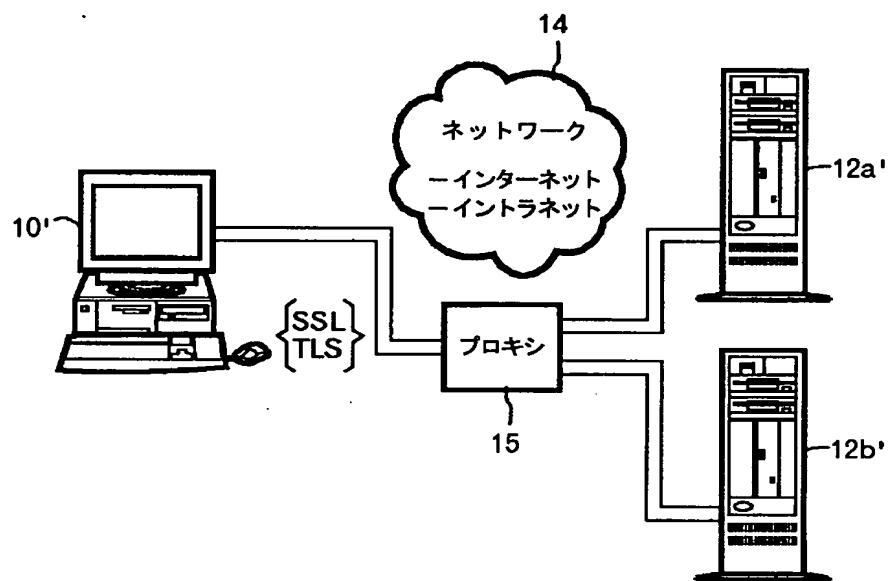
【図6】

本発明を実施することができる、パーベイシブ・コンピューティング・クライアント／サーバ・アーキテクチャのブロック図である。

【図1】



【図2】



【図3】

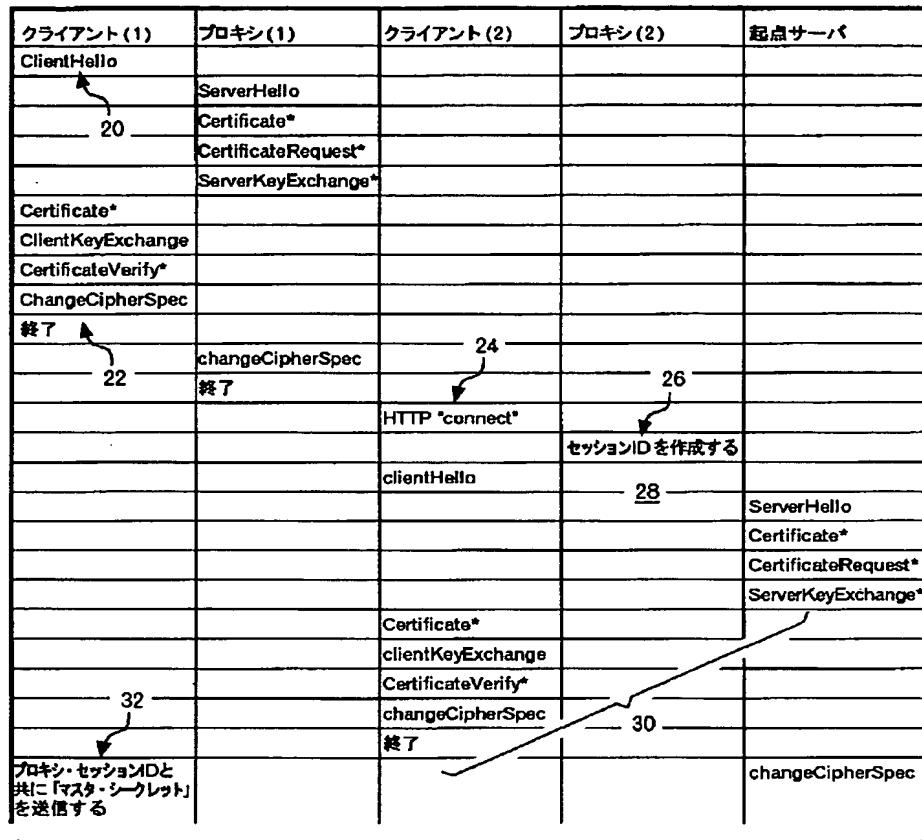


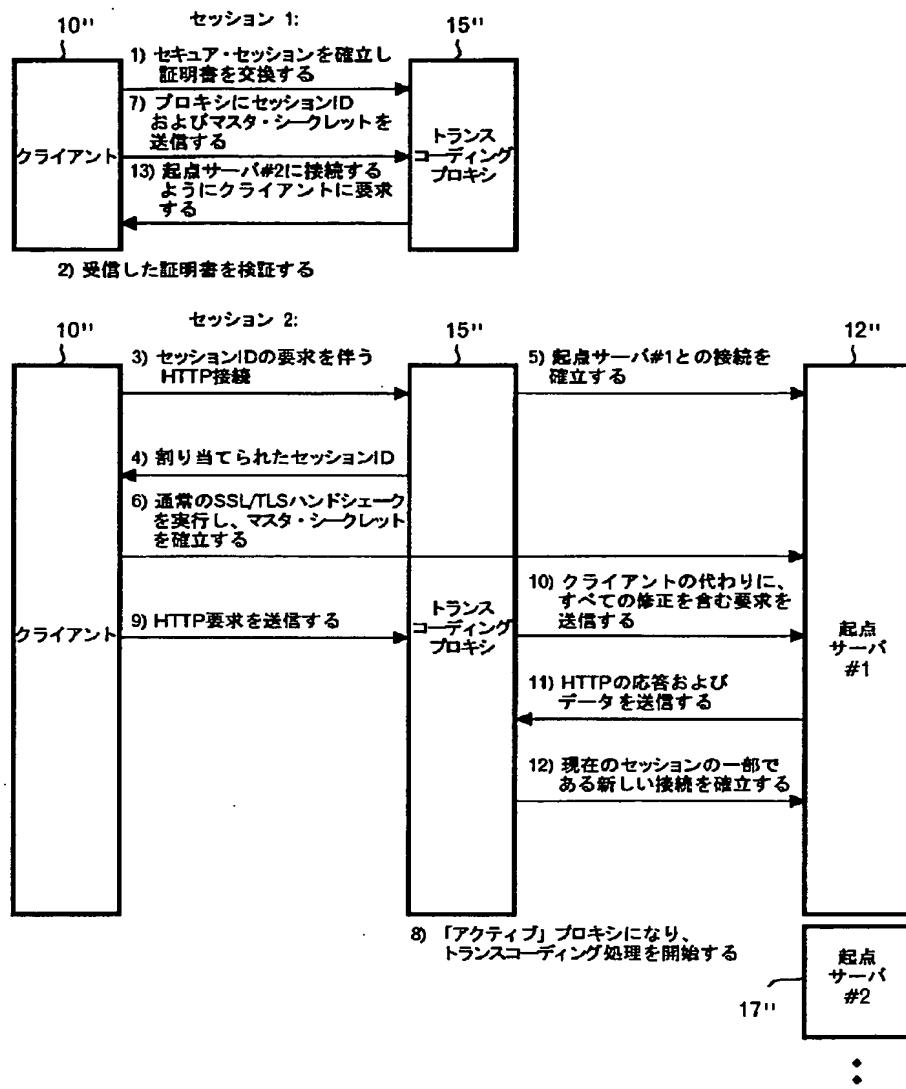
図4へ

【図4】

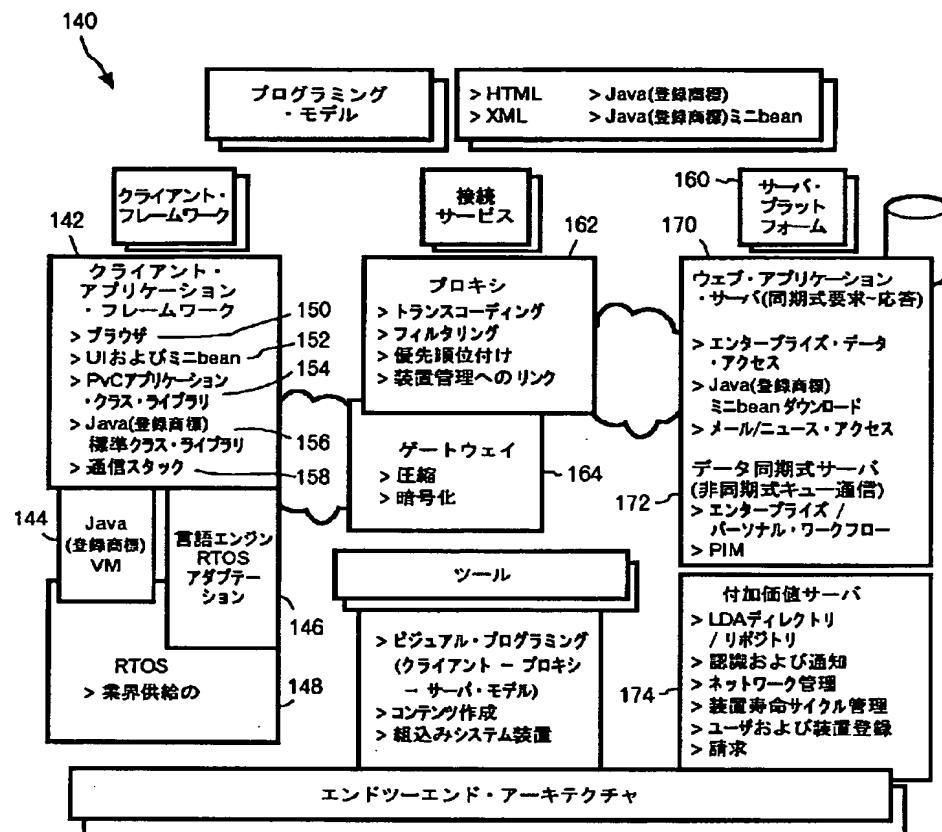
図3から

	「マスタ・シークレット」に基づいて暗黙ブロックを計算する		38	終了
34	HTTP要求	要求を更新/修正する	40	
36		HTTPコンテンツ応答		
	42	応答をトランスコードイングする		
		第2要求を送信する		HTTPコンテンツ応答
		(2)ClientHello 44		(2)ServerHello
				(2)Certificate*
				(2)CertificateRequest*
				(2)ServerKeyExchange*
				(2)Certificate*
				(2)ClientKeyExchange
				(2)CertificateVerify*
46		(2)changeCipherSpec		
		(2)終了		
	暗号仕様変更について クライアントに通知する		48	changeCipherSpec
changeCipherSpec				終了
終了		第3要求を送信する		HTTPコンテンツ応答
	50	最後の応答をトランスコードイングする		
		応答をレンダリングする		

【図5】



【図6】



## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

		Int. Search Application No PCT/GB 00/02469
A. CLASSIFICATION OF SUBJECT MATTER IPC 7 HO4L29/06		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 7 HO4L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the International search (name of data base and, where practical, search terms used) EPO-Internal, PAJ, WPI Data, IBM-TDB, INSPEC		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>NORIFUSA M: "Internet security: difficulties and solutions" COMMON SECURITY SOLUTIONS FOR COMMUNICATING PATIENT DATA. IMIA WORKING GROUP 4 WORKING CONFERENCE, OSAKA/KOBE, JAPAN, 22-25 NOV. 1997, vol. 49, no. 1, pages 69-74, XP004149463 International Journal of Medical Informatics, March 1998, Elsevier, Ireland ISSN: 1386-5056 pag 71-73, 5. SOKS version 5</p> <p>-/-</p>	1-25
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		<input checked="" type="checkbox"/> Patent family members are listed in annex.
<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published no or after the International filing date</p> <p>"L" document which may (have doubts on priority, claims) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the International filing date but later than the priority date claimed</p> <p>"T" later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"a" document member of the same patent family</p>		
Date of the actual completion of the International search	Date of mailing of the International search report	
2 March 2001	13/03/2001	
Name and mailing address of the ISA European Patent Office, P.O. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax. (+31-70) 340-3015	Authorized officer Bertolissi, E	

Form PCT/ISA/210 (second sheet) (July 1992)

## INTERNATIONAL SEARCH REPORT

Int'l. Search Application No.
PCT/GB 00/02469

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HAN' R ET AL: "Dynamic adaptation in an image transcoding proxy for mobile Web browsing" IEEE PERSONAL COMMUNICATIONS, DEC. 1998, IEEE, USA, vol. 5, no. 6, pages 8-17, XP000790121 ISSN: 1070-9916 pag 8-10 abstract	1-25
A	FOX A ET AL: "Adapting to network and client variability via on-demand dynamic distillation" 7TH INTERNATIONAL CONFERENCE ON ARCHITECTURAL SUPPORT FOR PROGRAMMING LANGUAGES AND OPERATING SYSTEMS, CAMBRIDGE, MA, USA, 1-5 OCT. 1996, vol. 31, no. 9, pages 160-170, XP000639230 SIGPLAN Notices, Sept. 1996, ACM, USA ISSN: 0362-1340 pag 160, 1 Introduction pag 168-169, 5 Related Work	1-25
A	WO 98 43177 A (INTEL CORP) 1 October 1998 (1998-10-01) abstract page 3, line 6 - line 14	1-25

## INTERNATIONAL SEARCH REPORT

Information on patent family members

Int'l. Appl. No.  
PCT/GB 00/02469

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9843177	A 01-10-1998	US 5902846 A	11-05-1999
		AU 6865698 A	20-10-1998
		BR 9811457 A	19-09-2000
		EP 1012733 A	28-06-2000

Form PCT/ISA210 (patent family entries) (July 1992)

## フロントページの続き

(51)Int.Cl.*	識別記号	F I	テーマコード(参考)
		H 04 L 9/00	601E

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW

(72)発明者 リタ、クリスチャン  
アメリカ合衆国78726 テキサス州オース  
チン アップルツリー・レーン 11101  
(72)発明者 ルツコスキー、マシュー、フランシス  
アメリカ合衆国78660 テキサス州フルジ  
ャービル クラレンス・ポールズ・レーン  
816

F ターム(参考) SB085 AA01 BC02  
SJ104 AA08 PA07 PA10  
SK030 GA08 GA15 HA08 HB18 HD03  
JA10 JA11 KX23 LD11 LD19  
MA09

## 【要約の続き】

ばトランスコーディング)を提供できるようになるための暗号情報を生成する。第2サーバからのデータが、第1サーバに対する所与のクライアント要求の処理中に必要になった場合には、プロキシが、同一のプロトコルを使用してプロキシを介して第2サーバにトンネリングする要求をクライアントに発行する。

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**